Health Information Service Provider (HISP)
Questions and Answers

1. What is a HISP?
   a. A HISP is a Health Information Service Provider, and the Kentucky Health Information Exchange has now implemented a HISP in support of the Transitions of Care objective found in Meaningful Use. The KHIE is offering both HISP services as well as Direct Secure Clinical messaging for participating providers. According to HealthIT.gov, being a service provider often means that HISPs have the ongoing responsibilities that often include:
      i. **Developing, maintaining and enforcing participation agreements**
      ii. **Providing online and phone support for onboarding, connectivity issues and outages, and other service needs**
      iii. **Assigning and managing (directly or through delegation) Direct domains and addresses**
      iv. **Provisioning, managing, and publishing certificates using DNS or LDAP**
      v. **Maintaining trust relations, possibly entailing joining a trust community and fulfilling its accreditation and other membership requirements**
      vi. **Ensuring Direct Security/Trust Agent (STA), certificate publication, and other customer supporting services are available and perform to the needs of customers**

2. Does KHIE support XDR (Cross-enterprise Document Reliable Interchange) for both incoming and outgoing messages with my organization?
   a. **Yes, KHIE supports XDR outgoing and incoming messages.**

3. Will KHIE allow for an organization-level certificate or does KHIE always require provider-level certificates?
   a. **KHIE supports organization level certificates.**

4. Will KHIE support the domain(s) I choose for my organization?
   a. **KHIE will support the domain(s) for each organization; however, approval is at the sole discretion of KHIE.**

5. Does KHIE maintain a provider directory?
   a. **KHIE maintains a Healthcare Provider Directory, which is populated with Direct email addresses.**

6. Does KHIE have any restrictions on how my organization can share my providers' Direct addresses with others?
   a. **KHIE does not restrict on how Direct addresses are shared.**

7. Will KHIE allow me to generate Direct addresses for my own users (within our agreed-upon domain)?

     a. **Yes, but KHIE requires organizations that use our HISP to perform identity proofing at National Institute of Standards and Technology (NIST) Level 3[1] of Assurance.**

8. Can KHIE support Direct addresses that I assign to departments or specialties rather than to specific users?

     a. **If you are managing your own direct users' accounts within your EHR, you have the ability to setup departments or specialties. KHIE routes messages based off the domain name. Setting up departments or specialties is based off your policy and procedures. Users must be identity proofed at NIST Level 3 Assurance.**

9. Do you require a provider at my organization to be registered with you before you will route messages for that address?

     a. **Organizations must have a participation agreement as well as a Direct addendum signed with KHIE. Organizations will need to provide a certificate to be added to our HISP if they are not using the KHIE-provided user interface. Identity proofing at NIST Level 3 Assurance must be completed before providers are able to send Direct messages.**

10. If a provider sends out a Direct message, but is unfamiliar with the sender, (although the sender has a Direct address in the same domain), will KHIE have any problem delivering it?

     a. **KHIE routes messages based off the domain name.**

11. If a provider receives a Direct message, and is unfamiliar with the recipient, but the recipient has a Direct address in the same domain, will KHIE deliver it to the provider?

     a. **KHIE routes messages based off the domain name.**

12. What do you do when you receive a message from/for a Direct address whose domain you do not trust?

     a. **Exchange must be performed through DTAAP, HISP to HISP connections, which are considered trusted domains. Therefore the message is not accepted for delivery.**

13. How do you handle the case where there is an organization that wants to exchange Direct messages, but are not yet connected to that organization's HISP or to the organization itself?

     a. **Connections to DTAAP approved HISPs will automatically be connected through Direct Trust Bundles. HISP to HISP connections, where the non-KHIE HISP has not completed DTAAP, will be at the discretion of the KHIE.**

---

[1] Level 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity proofing procedures require verification of identifying materials and information (NIST online).